Formal Analysis of Security Protocols
(Group: Crypto)

Presented by : Shruti Biswal

AERE/COMS 507X

May 2, 2017

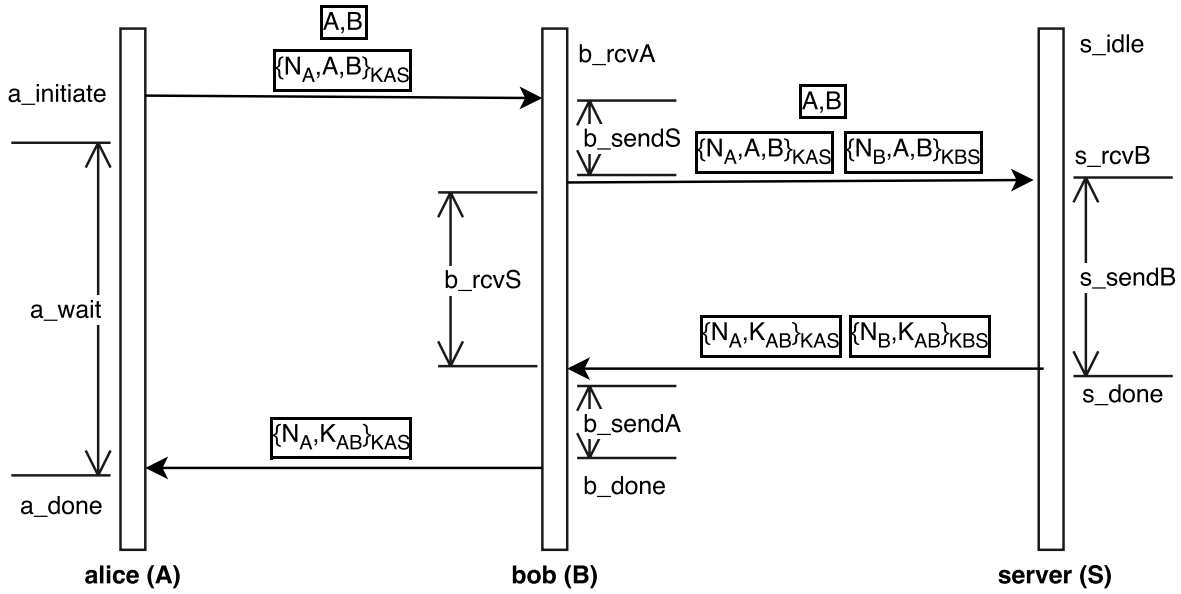
Motivation

- Security Protocols provide the basis for determining authenticated and authorized entities for safe transmission of information
- Need for Formal Analysis : To detect presence of any weakness in the protocol can lead to intrusion and thus, renders the protocol unsafe
- Where is the loophole ? : Most protocols establish the authentication and assume the communication channel to be secure.

Protocols Modelled For Attack Detection...

- Otway-Rees Protocol
- Needham - Schroeder Public Key Protocol
- Kerberos Protocol

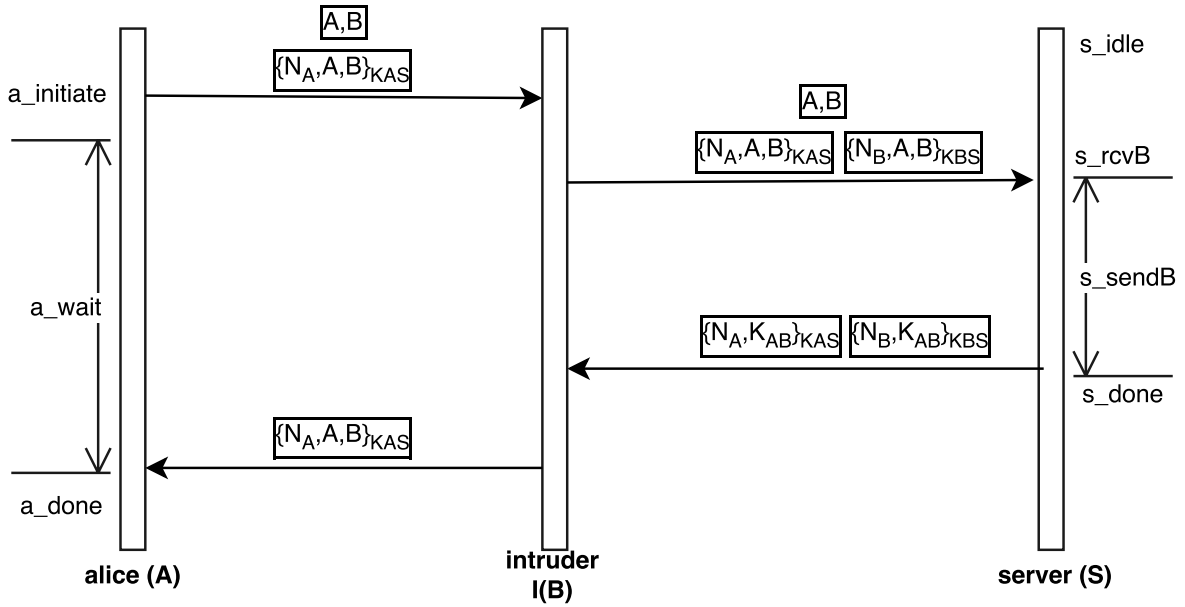
Otway-Rees Protocol



- It is always the case that if Agent A initiates a session then both Agent A and B should reach a state where session is successfully established.

Otway-Rees Model

Attack on Otway - Rees Protocol



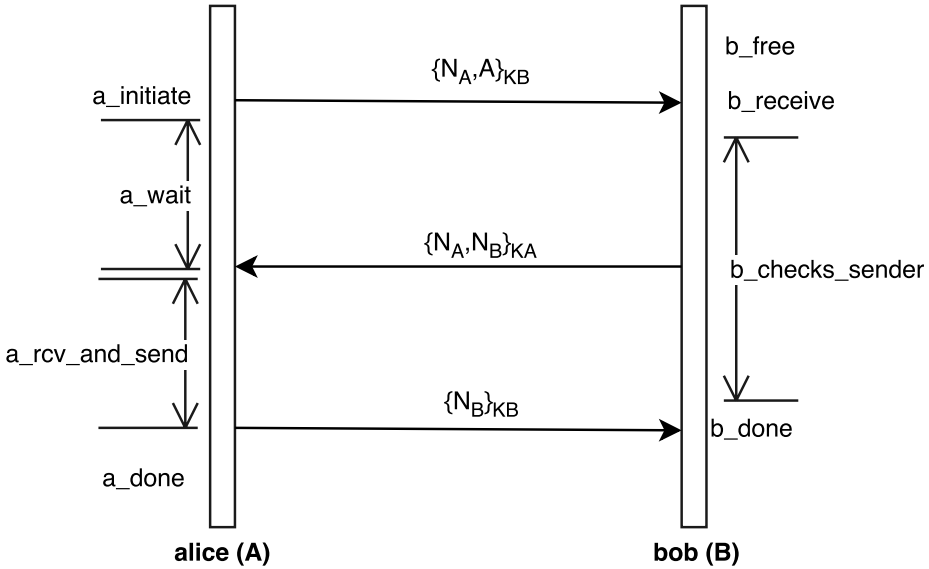
- Violates : If Agent A initiates a session then both Agent A and I(B) reach a state where session is successfully established and the intruder I(B) does NOT share a common key with A

Otway-Rees Model With Attack

Resolution for the Attack

- Can be resolved if the agent A in the last run expects to receive two packets where the first packet contains the encryption key for the second packet. In such scenario, the intruder I(B) cannot attack by re-sending an older message.

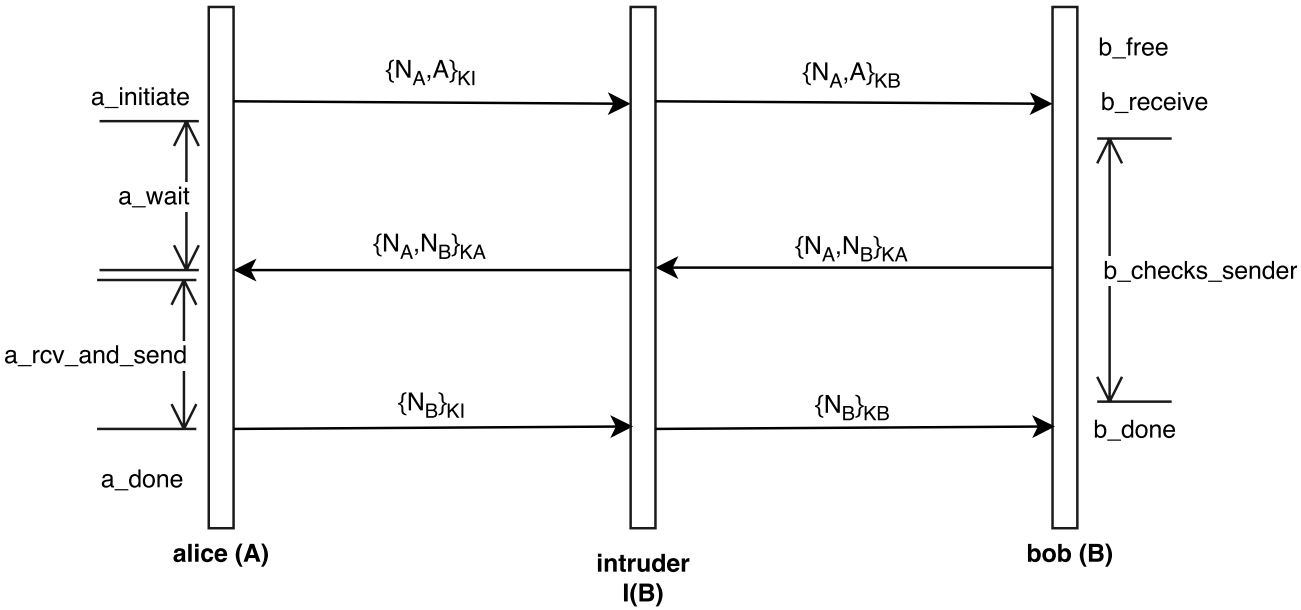
Needham Schroeder



- It is always the case that if Agent A initiates a session then both Agent A and B should reach a state where session is successfully established.

Needham Shcroeder Model

Attack on Needham Schroeder Protocol



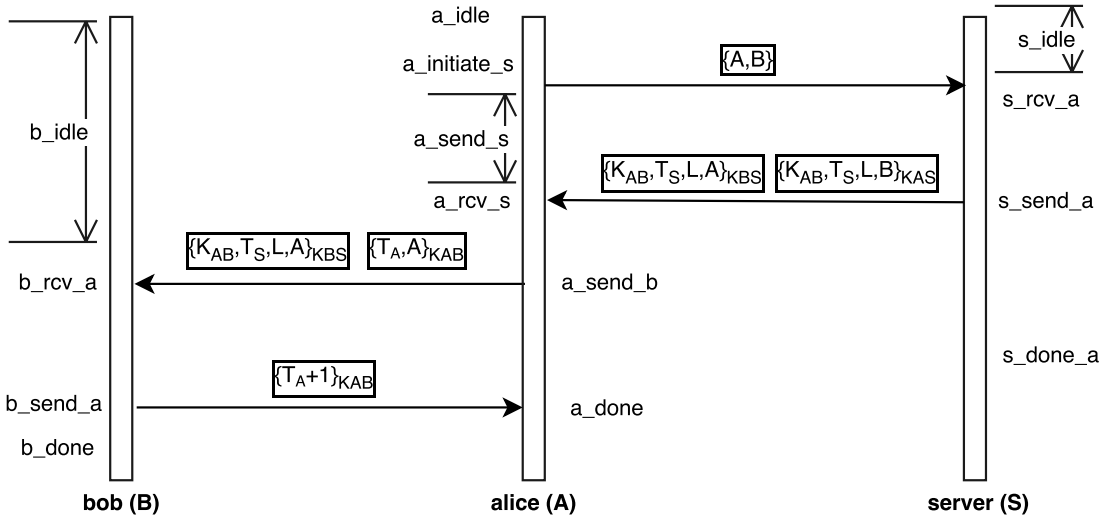
- Violates : If Agent A initiates a session then both Agent A and B reach a state where session is successfully established and the intruder I does NOT have the secret information from A and B

Needham Schroeder Model With Attack

Resolution for the Attack

- The attack was of type impersonation where the intruder pretended to be agent A with agent B.
- Can be resolved if agent B sends its identifier to I, which would further require A to receive an identifier for I (which he cannot generate due to the encryption key).

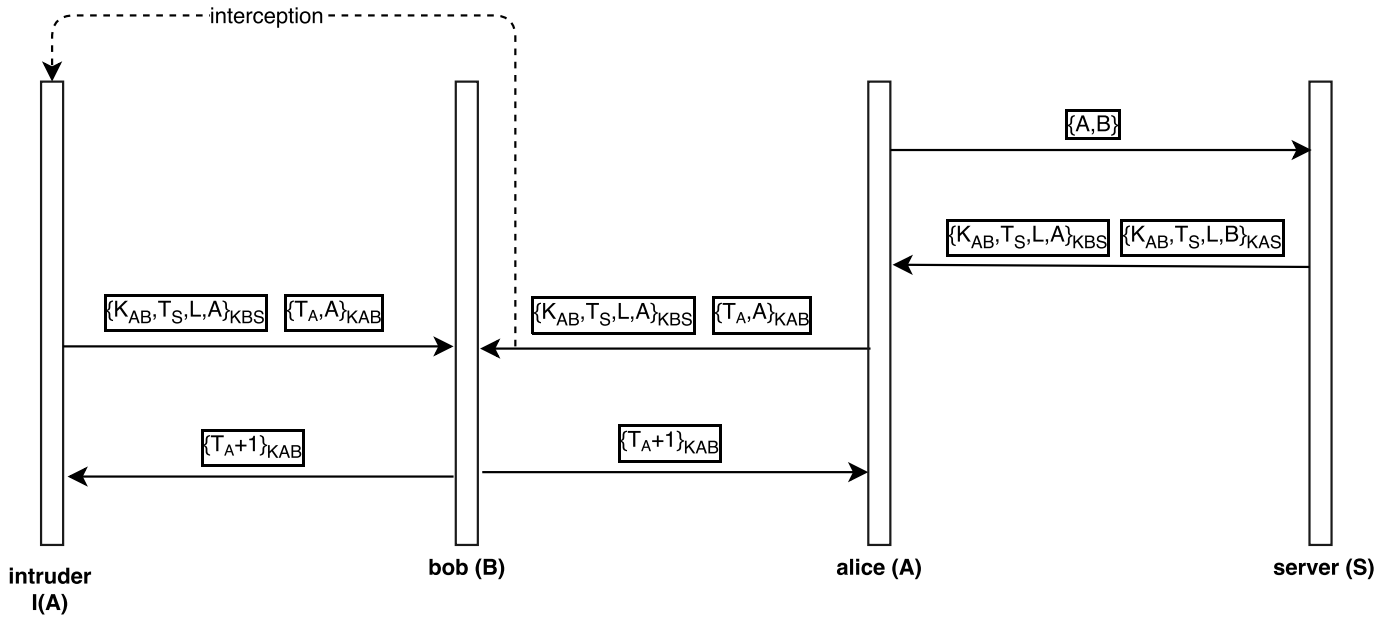
Kerberos Protocol



- **Authentication** : It is always the case that the number of sessions started by Agent A with B >= Number of sessions Agent B accepts with A.
- **Secrecy and Integrity**: Number of session keys shared by Agent A with B is >= Number of session keys Agent B accepts from A.

Kerberos Model

Attack on Kerberos Protocol



- **Authentication**: It is always the case that the number of sessions started by Agent I with B >= Number of sessions Agent B accepts with I.
- **Secrecy and Integrity**: Number of session keys shared by Agent I with B >= Number of session keys Agent I accepts from A.

Kerberos Model With Attack

Resolution for the Attack

- The attack was of type replay where the imposter set up a duplicate session with agent B and contacted B earlier than the honest agent A
- Can be resolved if agent B stores all the incoming authenticators from all the live sessions to detect replay.

Conclusion

- Formal analysis of security protocols to detect attack done via introduction of an all-powerful intruder who can eavesdrop, relay or imposter into the protocol model.
- Violation of security property like authentication or secrecy signify the presence of attack.
- Improvements or changes to the protocol help resolve the attack but may also be still vulnerable to a different kind of attack.

References

G. Lowe.

Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In Proceedings of TACAS, volume 1055 of Lecture Notes in Computer Science, pages 147–166. Springer Verlag, 1996.

M. Panti, L. Spalazzi, and S. Tacconi.

Using the NuSMV model checker to verify the kerberos protocol. [Online].
Available:http://www.inform.unian.it/personale/spalazzi/repo , 2002

Gizela Jakubowska, and Wojciech Penczek.

Modeling and Checking Timed Authentication of Security Protocols. Proceedings of the 2004 ACM Workshop on Formal Methods in Security Engineering, 23–32, FMSE '04

Frederic Massicotte

Man-in-the-middle attack against security protocols. Global Information Assurance Certification Paper, 2002